Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

34 413

Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)

Nr. 5

VERSLAG
Vastgesteld 1 april 2016

De vaste commissie voor Economische Zaken, belast met het voorbereidend onderzoek van bovengenoemd wetsvoorstel, heeft de eer als volgt een verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering de vragen en opmerkingen in dit verslag afdoende zal beantwoorden, acht de commissie hiermee de openbare behandeling van het voorstel van wet voldoende voorbereid.

Inhoudsopgave **blz.**

kst-34413-5
ISSN 0921 - 7371
’s-Gravenhage 2016

I. ALGEMEEN

De leden van de VVD-fractie hebben kennis genomen van het wetsvoorstel Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) en kunnen zich vinden in de algemene lijn van wetsvoorstel. Zij hebben nog een aantal vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden hebben nog enkele vragen en opmerkingen.

De leden van de SP-fractie hebben kennis genomen van het wetsvoorstel en hebben hierbij enkele vragen.

De leden van de CDA-fractie hebben kennisgenomen van onderhavig wetsvoorstel. De leden hebben nog enkele vragen en opmerkingen

De leden van de PVV-fractie hebben met ongenoegen kennisgenomen van voorliggend wetsvoorstel en willen de regering nog enkele vragen voorleggen.

De leden van de D66-fractie hebben met interesse kennisgenomen van het voorstel tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening vertrouwensdiensten). Zij hebben nog enkele vragen en opmerkingen.

1. Inleiding

De leden van de PvdA-fractie lezen dat bij dit wetsvoorstel uitgegaan wordt van minimumomzetting, in verband met de rechtstreekse werking van de verordening 910/2014. Deze leden zijn dan enigszins verbaasd dat, nu uitgegaan wordt van de rechtstreekse werking van de verordening, er toch 19 bladzijden aan wettekst nodig is om de Nederlandse wet aan te passen. Hoe verhoudt dit zich tot elkaar?
De verordening en de wet vormen tezamen een samenhangend stuk wetgeving. Uitgaan van rechtstreekse werking van verordening kan echter ten koste gaan van de overzichtelijkheid en inzichtelijkheid van wetgeving voor ondernemers en consumenten. Hoe gaat de regering dit probleem ondervangen? Zal op de website van het ministerie inzichtelijk gemaakt worden hoe de nieuwe wet- en regelgeving rondom elektronische identiteiten en vertrouwensdiensten eruit komt te zien? Op welke websites en van welke departementen zal dit inzichtelijk gemaakt worden?
Er horen meerdere maatregelen van bestuur bij dit wetsvoorstel. Waarom worden deze niet voorgehangen bij de Kamer, zo vragen deze leden.

De leden van de CDA-fractie vragen de regering of de voorstellen zijn getoetst aan de hand van het subsidiariteitsbeginsel. Zo ja, zijn er volgens de regering artikelen die beter nationaal zouden kunnen worden geregeld? Daarnaast vragen deze leden of de regering kan bevestigen dat bij de omzetting van Europese regelgeving de regering alleen datgene heeft omgezet wat strikt genomen op grond van de Europese regelgeving noodzakelijk is. Deze leden vragen verder of dit wetsvoorstel eraan bijdraagt dat Nederlandse bedrijven internationaal met aanbestedingen mee kunnen doen en of het makkelijker wordt om in Europa vergunningen aan te kunnen vragen. Zo ja, op welke wijze draagt het wetsvoorstel hiertoe bij? Verder lezen deze leden in het verslag van het Verzamel algemeen overleg Telecommunicatie op 21 november 2012 (Kamerstuk 24 095, nr. 327) dat Nederland zich bij het overleg over de totstandkoming van de verordening vooral zal gaan richten op uitvoerbaarheid, veiligheid, effectief toezicht en de aansprakelijkheid van de Staat, waarvan mogelijk sprake zou kunnen zijn. Zou de regering kunnen aangeven wat Nederland wel en niet heeft binnengehaald bij het overleg over de totstandkoming van de verordening? En zou de regering nader kunnen toelichten waarom dit voorstel uitvoerbaar is? Tevens vragen deze leden of dit wetvoorstel gevolgen heeft voor inwoners die het lastig vinden om mee te komen met de digitale wereld. Zo ja, om welke gevolgen gaat het en in hoeverre bestaan er voor deze groepen inwoners alternatieven? Tot slot vragen deze leden of de regering aan zou kunnen geven waarom er voor gekozen is om in de wet geen evaluatiebepaling op te nemen en waarom bij de algemene maatregelen van bestuur in het wetsvoorstel geen voor- en/of nahangbepalingen zijn opgenomen.

De leden van de PVV-fractie bespeuren geen enkele dosis wantrouwen jegens buitenlandse elektronische identiteiten en vertrouwensdiensten. Waar is dit vertrouwen op gebaseerd? Nota bene het eigen Nederlandse DigiD-systeem is in het verleden dikwijls in opspraak gekomen, omdat het een onbetrouwbaar zooitje zou zijn. Waarom zouden nu blindelings moeten worden vertrouwd op de elektronische identificatiemiddelen van

andere lidstaten? Kan Nederland als lidstaat zelf niet bepalen welk elektronisch identificatiemiddel betrouwbaar is en welke middelen niet? Verder zijn deze leden ook benieuwd naar de implicaties van dit wetsvoorstel. Deze leden herinneren de regering aan het feit dat criminelen met behulp van fraude met DigiD honderden euro's huur, zorg en kinderopvangtoeslagen hebben weten te bemachtigen. Nu is deze regering nogal kwistig met het strooien van Nederlands belastinggeld aan andere lidstaten, maar zet dit de deur niet helemaal wagenwijd open voor misbruik van onze sociale voorzieningen? Deze leden ontvangen dan ook graag een overzicht van de publieke diensten waar deze verplichte erkenning van elektronische identificatiemiddelen van toepassing wordt. Verder begrijpen deze leden dat deze elektronische identificatie ook gebruik gaat worden voor elektronische transacties. Betekent dit bijvoorbeeld dat Nederlandse burgers met hun elektronische identificatie (zoals een DigiD of vergelijkbaar systeem) straks bij een Poolse webwinkel goederen kunnen aanschaffen, ja of nee?

2. De eidas-verordening en gerechtvaardigd vertrouwen bij digitaal verkeer

2.1 Elektronische identificatie en elektronische identificatiemiddelen

De leden van de VVD-fractie lezen op pagina 4 van de memorie van toelichting dat elektronische identificatie wordt gedefinieerd als een proces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt. Deze leden vragen in hoeverre er daarbij nadere eisen worden gesteld aan het inrichten van de beheerprocessen binnen een ICT-organisatie, zoals die benodigd is voor het opstellen en uitgeven van elektronische identiteiten en vertrouwensdiensten. Kan de regering daar een nadere toelichting op geven? Worden er bijvoorbeeld kaders voor het inrichten van beheerprocessen voorgeschreven? Deze leden denken bijvoorbeeld aan kaders als een Information Technology Infrastructure Library (ITIL).

2.2 Vertrouwensdiensten

De leden de CDA-fractie vragen in hoeverre de in het wetsvoorstel genoemde vertrouwensdiensten nog kinderziektes bevatten. Is het gebruik van de vertrouwensdiensten volledig veilig?

2.3 Certificaten onderdeel van vertrouwensdiensten

De regering stelt dat het op afstand verkrijgen van een gekwalificeerd certificaat voor natuurlijke personen en rechtspersonen met deze wetswijziging in de praktijk eenvoudiger wordt. De leden van de D66-fractie juichen dit toe, maar stellen vast dat de verificatie van de identiteit in fysieke aanwezigheid moet plaatsvinden. Is dat onder de huidige regelgeving ook het geval? Indien nee, is er dan wel sprake van een vereenvoudiging van het verkrijgen van een gekwalificeerd certificaat? Daar de verordening deze procedure uitdrukkelijk bij de EU-lidstaten zelf laten, is er geen mogelijkheid voor Nederland om voor natuurlijke personen en rechtspersonen ook slechts via een elektronische procedure een gekwalificeerd certificaat aan te vragen?

3. De inhoud en uitvoering van de eidas-verordening op hoofdlijnen

3.1 Inhoud eidas-verordening op hoofdlijnen

De leden van de PVV-fractie begrijpen dat een goed functionerend elektronisch identificatiesysteem steeds belangrijker wordt. De leden willen de regering er echter op wijzen dat in de verschillende lidstaten anders wordt gedacht over de betrouwbaarheid van de publieke instellingen. Zeker in zuidelijke en Oost-Europese lidstaten is er sprake van een groot wantrouwen jegens de eigen overheid, kijk bijvoorbeeld maar naar de belastingmoraal van de Grieken. In hoeverre is het dan verantwoord om buitenlandse overheidsdiensten die zelfs door de eigen bevolking niet vertrouwd worden toegang te verlenen tot de elektronische identificatiegegevens van Nederlandse burgers? Verder zijn deze leden benieuwd in hoeverre deze verordening een verplichting wordt voor onze Nederlandse burgers die in een andere Europese lidstaat iets willen regelen. Met andere woorden stel dat een Nederlander in Athene wil studeren of daar belastingaangifte moet doen, kan dat straks dan alleen nog maar via een elektronisch identificatiesysteem (zoals DigiD of de opvolger daarvan)? Daarnaast vormt dit systeem omgekeerd ook een inbreuk op onze verzorgingsstaat, doordat het voor iedere Bulgaar of Roemeen een stuk eenvoudiger wordt om aanspraak te maken op bepaalde toeslagen en subsidies. De praktijk heeft immers al uitgewezen dat met name Oost-Europeanen erg behendig zijn in het maximaal uitbuiten van onze verzorgingsstaat. Zelfs al zou men op legitieme wijze aanspraak kunnen maken op één van onze sociale voorzieningen, acht de regering het dan wenselijk om dit te faciliteren? Zo niet, hoe wil de regering onder dit systeem voorkomen dat burgers van andere lidstaten steeds vaker een beroep doen op door met Nederlands belastinggeld gefinancierde sociale voorzieningen? Ook voor wat de privacy en veiligheid betreft hebben deze leden forse bedenkingen. Het is natuurlijk ook merkwaardig dat de Nederlandse overheid actief adviseert om niet overal een kopie van je paspoort achter te laten, terwijl de elektronische identificatie van burgers straks overal rondslingert. Dat zal ongetwijfeld gebonden zijn aan allerlei strenge regels, maar waar burgers bij een kopie van het paspoort nog altijd zelf het BSN nummer kunnen doorkrassen of het kopietje kunnen terugvragen bij vertrek hebben burgers geen zicht wat er met een eenmalig verleende toegang tot het elektronische identificatiesysteem gebeurt. Kan de regering aangeven hoe een Nederlandse burger straks kan controleren wie er toegang heeft tot zijn of haar elektronische identificatie? En kan de regering ook aangeven hoe een Nederlandse burger deze toegang eenzijdig kan intrekken, wijzigen of blokkeren?

De leden van de D66-fractie lezen dat «een lidstaat niet verplicht is tot het aanmelden van een stelsel bij de Europese Commissie over te gaan om erkenning te bewerkstelligen». Kan de regering nader toelichten wat met deze zinsnede bedoeld wordt?

3.2 Voorgestelde uitvoering eidas-verordening op hoofdlijnen

De leden van de D66-fractie lezen dat het knooppunt dat dient tot grensoverschrijdende acceptatie van elektronische identificatiemiddelen in september 2018 gereed dient te zijn. Kan de regering aangeven of deze deadline gehaald gaat worden? Is er al een aanbestedingsprocedure gestart? Is de regering zich bewust van de complexiteit van zowel de ontwikkeling als het onderhoud van een dergelijk knooppunt, zoals genoemd in het advies van het Cbp? Hoe wordt dit advies meegenomen in de ontwikkeling van het knooppunt?

4. Erkenning elektronische identificatiemiddelen

4.1 Grensoverschrijdende erkenning elektronische identificatiemiddelen

De leden van de PvdA-fractie vragen of het klopt dat de rechtsgevolgen van de gekwalificeerde elektronische handtekening tot nu toe worden geregeld in artikel 3:15a van het Burgerlijk Wetboek. Welke meerwaarde heeft het om dit te schrappen voor de gekwalificeerde elektronische handtekening?
Kan de regering aangeven wat de verschillen en overeenkomsten zijn tussen de geavanceerde, gekwalificeerde en andere elektronische handtekeningen? Welke technische verschillen zijn er en welke verschillen in rechtsgevolgen?
Deze leden vragen hoe wordt bepaald of een elektronische handtekening voldoende betrouwbaar is in de zin van het voorgestelde artikel 2:16 van de Algemene wet bestuursrecht (Awb). In welke nadere regelgeving wordt dit vastgesteld? Waar zal worden geregeld welke aanvullende eisen zullen worden gesteld, zoals bedoeld in artikel 2:16, tweede lid, van de Awb?

De leden van de SP-fractie lezen dat de verplichting tot erkenning van elektronische identificatiemiddelen is beperkt tot middelen met minimaal het substantiële betrouwbaarheidsniveau. Deze leden zijn benieuwd naar de hiermee gepaard gaande risico's en vragen naar een voorbeeld van een dienst die zich aan de onderkant bevindt van het substantiële betrouwbaarheidsniveau.

De leden van de PVV-fractie zijn benieuwd hoe het Nederlandse Agentschap Telecom gaat toetsen of een buitenlands elektronisch identificatiemiddel met een zogenaamd substantieel of hoog betrouwbaarheidsniveau in de praktijk ook daadwerkelijk aan deze betrouwbaarheidseisen voldoet. Of is het zo dat indien een instantie eenmaal de status van hoge betrouwbaarheid heeft behaald binnen een lidstaat van de Europese Unie, de Nederlandse toezichthouder verder niet meer controleert of dit ook daadwerkelijk zo is?

4.2 Uitvoeringsmaatregelen

De leden van de PvdA-fractie vragen wat de stand van zaken met betrekking tot het knooppunt dat grensoverschrijdende identificatie mogelijk maakt, dat in september 2018 gereed zou zijn. Wanneer zal de bijbehorende Privacy Impact Assessment aan de Kamer worden verstuurd? Klopt het dat het Cbp (Autoriteit Persoonsgegevens) geadviseerd heeft deze uit te voeren? Is de benodigde extra informatie die volgens het Cbp nodig is inmiddels beschikbaar? Komen er aanvullende Privacy Impact Assessments? Zo ja, wanneer?
Deze leden vragen waar dit knooppunt komt. Welke landen gaan deelnemen aan dit eIDAS-knooppunt? Zijn dit ook landen als Roemenië en Bulgarije? Wat gebeurt er als de toekenning van elektronischer identiteiten daar lek is (d.w.z. vervalste identiteiten, identiteitsdiefstal, etc.)? Is het dan niet zo dat de identificatieproblemen van andere landen in Nederland worden geïmporteerd?
Is inmiddels zeker gesteld dat dit knooppunt geen gegevens kan en mag opslaan, zo vragen deze leden. Hoe worden storingen bij het knooppunt ondervangen?

De leden van de SP-fractie lezen dat via het met deze wet ingestelde knooppunt verbinding wordt gemaakt met het stelsel voor elektronische identiteit (eID-stelsel). Deze leden zijn benieuwd naar de risico's die een buitenlands middel met een vrij laag betrouwbaarheidsniveau dat verplicht erkend moet worden in het eID-stelsel kan introduceren, welke

mogelijkheden er zijn om dit middel te weren en welke voorzorgsmaatregelen hiertegen worden voorbereid. Daarnaast willen deze leden weten op welke wijze de Minister van Economische Zaken met de Minister van Binnenlandse Zaken zal samenwerken om deze risico's uit te bannen.

De leden van de PVV-fractie vinden de volgordelijkheid wat merkwaardig. De Kamer wordt nu al gevraagd om in te stemmen met automatische erkenning van elektronische identificatiemiddelen van Europese lidstaten, terwijl de benodigde technische voorziening nog gerealiseerd moet worden. Klopt het dat de Kamer zelfs nog moet beslissen of dat nieuwe eID-stelsel wel wenselijk is en wat de reikwijdte ervan is?

4.3 De melding van een stelsel tot bewerkstelliging van erkenning

De leden van de D66-fractie lezen dat «de aanmeldende lidstaat [dient] te voorzien in de werking en beschikbaarheid van een online authenticatievoorziening». Bedoelt de regering hiermee dat elk lidstaat apart in een authenticatievoorziening, een knooppunt, moet voorzien? Zo ja, ziet de regering mogelijkheden om het aanbesteden van een dergelijk knooppunt via open source software te laten verrichten zodat niet 28 keer dezelfde software hoeft te worden aanbesteed? Is erover nagedacht, en is het mogelijk, om in plaats van 28 afzonderlijke knooppunten één knooppunt te creëren?

4.4 Uitvoeringsmaatregelen

De leden van de D66-fractie stellen vast dat er nog geen uitsluitsel is over de vraag of en wanneer Nederland een stelsel voor elektronische identificatie gaat aanmelden voor wederzijdse erkenning. Kan de regering aangeven welke huidige en toekomstige middelen voor een dergelijk stelsel in aanmerking komen?
Voorts lezen deze leden dat de totstandkoming van een dergelijk stelsel afhangt van nationale ontwikkelingen, zoals de totstandkoming van een stelsel voor elektronische identificatie (Idensys). Kan de regering aangeven in hoeverre de voortgang van de ontwikkelingen van Idensys samenhangt met de uitvoering van dit wetsvoorstel? Daarnaast zijn deze leden benieuwd welke andere nationale ontwikkelingen invloed hebben op een eventuele Nederlandse aanmelding voor wederzijdse erkenning.

5. Het verlenen van vertrouwensdiensten

5.3 Meldplichten bij inbreuk op veiligheid of verlies van integriteit

De leden van de D66-fractie constateren dat volgens de regering aanbieders van gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten verplicht zijn een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd vierentwintig uur na ontdekking te melden. Dit moet gedaan worden bij het door een lidstaat aangewezen toezichthoudend orgaan van de lidstaat waar de verlener gevestigd is. Hoewel deze leden het goed vinden dat deze verplichting er is, zouden zij graag concreter willen weten wanneer gevolgen «aanzienlijk» zijn. Kan de regering het begrip «aanzienlijk» definiëren en aangeven waarom niet alle veiligheidsinbreuken of integriteitsverliezen gemeld moeten worden?

Deze leden lezen daarnaast dat indien het algemeen belang daarmee wordt gediend, het toezichthoudend orgaan kan bepalen dat het publiek wordt of moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Kan de regering aangeven of hier een protocol voor

wordt opgesteld? Zo nee, waarom niet? Zo ja, kan de regering aangeven wat de voortgang hiervan is en het «algemeen belang» definiëren?

5.4 Uitvoeringsmaatregelen

De leden van de PvdA-fractie constateren dat de Minister van Veiligheid en Justitie wordt aangewezen als het nationale orgaan van informatieveiligheid. In hoeverre verandert dit de situatie in vergelijking met de situatie tot nu toe? De Autoriteit Persoonsgegevens (tot voor kort Cbp) wordt aangewezen als gegevensbeschermingsautoriteit. In hoeverre verandert dit de situatie in vergelijking met de situatie tot nu toe?

De leden van de D66-fractie stellen vast dat er alleen in Nederland al meerdere organen zijn waar verschillende inbreuken gemeld kunnen worden: de Autoriteit Persoonsgegevens, het Agentschap Telecom (AT), de Autoriteit Consument en Markt (ACM) en het Nationaal Cyber Security Centrum (NCSC). Zorgen over een grote hoeveelheid organen waaraan inbreuken gemeld moeten worden, werden ook uitgesproken door een respondent tijdens de internetconsultatie (zie paragraaf 13 van de memorie van toelichting), waarop de regering aangeeft dat een samenwerkingsverplichting voor AT, NCSC, en Cbp in het wetsvoorstel wordt opgenomen: «zij zijn verplicht een samenwerkingsprotocol af te sluiten in het belang van effectieve en efficiënte meldingen op grond van de verordening en over het toezicht als een melding ook een inbreuk op persoonsgegevens betreft». Kan de regering dit nader toelichten? Kan de regering door middel van een tabel een overzicht geven van de verschillende types meldplichten? Heeft de regering nagedacht over het opzetten van één loket voor de bovengenoemde meldplichten?

5.5 Gekwalificeerde vertrouwensdiensten en vertrouwenslijsten

Op grond van artikel 19 van de verordening zijn aanbieders van vertrouwensdiensten verplicht een veiligheidsbreuk binnen 24 uur te melden aan het toezichthoudend orgaan, zo leden de leden van de PvdA-fractie. Dit geldt ook voor integriteitsverlies met aanzienlijke gevolgen. Wat zijn in dit geval «aanzienlijke gevolgen»? Welke instantie gaat het begrip «aanzienlijke gevolgen» nader invullen? Is dit vanaf nu het Agentschap Telecom, in plaats van de ACM? Leidt dit ook tot een overplaatsing van personeel naar het Agentschap Telecom?

De leden van de PVV-fractie zijn benieuwd of het toezichthoudend orgaan in Nederland gekwalificeerde dienstverleners uit andere EU-lidstaten met een vertrouwensmerk van de Europese Unie nog op enigerlei wijze controleert. Of is het zo dat indien een dienstverlener eenmaal over dit Europese vertrouwenskenmerk beschikt hij automatisch op de vertrouwenslijst van iedere lidstaat moet worden opgenomen?

5.6 Uitvoeringsmaatregelen

De leden van de PvdA-fractie vragen of bij DigiNotar in 2011 ook sprake was van een veiligheidsbreuk en integriteitsverlies met aanzienlijke gevolgen. Is dit toen ook binnen 24 uur gemeld aan een toezichthoudend orgaan? Zou de afwikkeling van het DigiNotar-lek met dit wetsvoorstel op een andere manier gebeuren dan tot nu toe?
In artikel 18.7 worden de Nederlandse eisen aan certificatiedienstverleners geschrapt, omdat de Eidas-verordening zelf eisen hieraan stelt. Deze leden vragen wat de verschillen en overeenkomsten zijn tussen de Nederlandse en Europese eisen?

5.7 Toezicht en handhaving

De leden van de CDA-fractie lezen dat lidstaten verplicht zijn om voorschriften vast te stellen inzake de sancties die van toepassing zijn op inbreuken op de verordening en daarmee ook ten aanzien van vertrouwensdiensten. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. Hoe wordt dat in Nederland ingericht? In het wetsvoorstel lezen deze leden dat aanbieders van gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst, of voor de persoonsgegevens die daarmee worden beheerd, binnen 24 uur na ontwikkeling moeten melden. Deze leden vragen hoe de regering zich dat voorstelt? Zou de regering kunnen aangeven hoe zij dit concreet wil gaan uitwerken en of dit uitvoerbaar is? Deze leden zouden graag zien dat de regering hierbij specifiek ingaat op de handhaving. Zij vragen de regering of er sancties gelden indien er niet tijdig wordt gemeld en zo ja welke sancties dit zijn. Tot slot vragen deze leden of het klopt dat het toezicht en handhaving op gekwalificeerde certificaten voor elektronische handtekeningen wordt weggehaald bij de ACM. Zo ja, waarom?

5.8 Uitvoeringsmaatregelen

De leden van de VVD-fractie lezen op pagina 23 van de memorie van toelichting dat periodieke conformiteitsbeoordeling een belangrijke rol blijft spelen en dat de audit daarvoor door een conformiteitbeoordelingsinstantie wordt uitgevoerd die daarbij een andere rol en verantwoordelijkheid heeft dan de toezichthouder. Deze leden kunnen zich goed vinden in het feit dat het eindoordeel wordt gevormd door de toezichthouder en dat dit de eigen oordeelsvorming niet kan en mag vervangen. Deze leden vragen in hoeverre het instrument «audit» door de conformiteitsbeoordelingsinstantie in dit stelsel ter ondersteuning van de naleving voldoende is uitgewerkt. Kan de regering daar een toelichting op geven? Is de regering ervan op de hoogte dat uit de parlementaire enquête Fyra bleek dat het begrip «audit» onvoldoende was gedefinieerd om daarop te kunnen steunen?

De leden van de PvdA-fractie vragen waarom artikel 18.16a van de Telecommunicatiewet over het vermoeden van overeenstemming vervalt.

De leden van de D66-fractie constateren dat de regering het wenselijk acht dat er een Europees conformiteitsbeoordelingsschema wordt ontwikkeld om harmonisatie van conformiteitsbeoordelingen en -verslagen tussen lidstaten te bewerkstelligen. Toch stellen deze leden vast dat het gebruik van een dergelijk Europees schema niet verplicht zal worden, omdat dat het niet wenselijk wordt geacht. De eerdergenoemde leden vragen of een Europees conformiteitsschema, ondanks dat het niet wenselijk is dat het gebruik van een dergelijk schema wettelijk verplicht wordt, toch wordt ontwikkeld. Zo ja, wat is de voortgang daarvan? Daarnaast willen deze leden graag meer uitleg over waarom een wettelijke verplichting tot gebruik van een dergelijk schema niet wenselijk is. Kan de regering hier meer over uitweiden, naast de korte uitleg die al gegeven wordt?

5.9 Aansprakelijkheid

De leden van de PvdA-fractie vragen of het klopt dat voor gekwalificeerde verleners van vertrouwensdiensten een omkering van de bewijslast geldt. Hoe verhoudt dit zich tot de omkering van de bewijslast (het rechtsvermoeden) uit de Mijnbouwwet?

De leden van de PVV-fractie constateren dat verleners van niet-gekwalificeerde vertrouwensdiensten niet de bewijslast dragen indien er schade wordt toegebracht aan een persoon vanwege het niet naleven van de verplichtingen uit deze verordening, terwijl dit voor gekwalificeerde verleners wel het geval is. Waarom is er voor deze constructie gekozen? Kan ook hier de bewijslast worden gelegd bij de verleners van de vertrouwensdiensten, ook al zijn ze niet gekwalificeerd? Hoe kan een Nederlandse burger controleren of een verlener van vertrouwensdiensten gekwalificeerd is of niet?

De leden van de D66-fractie stellen vast dat verleners van vertrouwensdiensten, onder bepaalde voorwaarden, beperkingen verbinden aan het gebruik van de door hen verleende diensten en dat zij niet aansprakelijk zijn voor schade die het gevolg is van het gebruik van diensten dat deze beperkingen te buiten gaat. De klanten moeten volgens de memorie van toelichting vooraf terdege worden geïnformeerd over de beperkingen. Kan de regering aangeven onder welke specifieke voorwaarden dergelijke beperkingen verbonden kunnen worden aan verleende diensten? Kan de regering daarnaast definiëren wanneer klanten «terdege» geïnformeerd worden?

5.10 Uitvoeringsmaatregelen

De leden van de PvdA-fractie constateren dat artikel 6:196b Burgerlijk Wetboek over de aansprakelijkheid van certificatiedienstverleners vervalt. In artikel 13 van de verordening staan hier nu regels over opgenomen. Welke verschillen en overeenkomsten zijn er nu tussen de Nederlandse en Europese regels?

5.11 Derde landen

De leden van de PvdA-fractie vragen of er op dit moment al veel overeenkomsten van de EU en derde landen over erkenning van certificatie zijn. Hoeveel van dergelijke overeenkomsten worden er voorzien?

5.13 Toegankelijkheid voor personen met een handicap

De leden van de SP-fractie lezen dat toegankelijkheid voor personen met een handicap aan technische en financiële mogelijkheden wordt gerelateerd. Deze leden zijn benieuwd naar de criteria die hiervoor worden opgesteld en op welke wijze vertrouwensdiensten met toegankelijkheid voor gehandicapten worden onderscheiden van anderen. Tevens zijn deze leden benieuwd welke belemmeringen bestaan om deze toegankelijkheid verplicht te stellen.

Voor overheden is het verplicht om te voldoen aan de webrichtlijnen, waarmee de toegankelijkheid ook voor mensen met een handicap wordt geborgd. Voor niet-overheden geldt deze regel niet. De leden van de CDA-fractie vragen waarom deze regel niet geldt voor niet-overheden. Tevens vragen deze leden in hoeverre bedrijven volgens de regering kunnen worden gestimuleerd om vertrouwensdiensten technisch toegankelijk te maken voor personen met een handicap.

6. Rechtsgevolgen bij gebruik van vertrouwensdiensten

6.1 Bewijs en rechtsgevolgen

De leden van de PVV-fractie constateren dat niet-gekwalificeerde vertrouwensdiensten niet automatisch erkend worden als toelaatbaar bewijsmiddel in gerechtelijke procedures, en niet ten onrechte. Echter

omdat niet-gekwalificeerde vertrouwensdiensten ook geen bewijslast hebben, vragen deze leden waarom überhaupt Nederlandse burgers gebruik zouden maken van een niet-gekwalificeerde vertrouwensdienst. Zou de regering juist Nederlanders niet moeten waarschuwen voor deze niet-gekwalificeerde vertrouwensdiensten?

6.2 Uitvoeringsmaatregelen

De regering geeft aan dat voor elektronische diensten anders dan de elektronische handtekening ons nationaal recht geen algemene regeling heeft over rechtsgevolgen of over het vermoeden van integriteit en juistheid. Wordt dit niet nodig geacht, zo vragen de leden van de D66-fractie. Zo nee, waarom? Zo ja, welke stappen worden ondernomen om dit juridisch vast te leggen?

7. Erkenning van vertrouwensdiensten

7.1 Erkenning van elektronische handtekeningen en zegels

De regering beschrijft dat voor gevolgen van ontwikkelingen op het internet zoals cloudoplossingen de omgeving waarin sleutelgegevens worden bewaard niet altijd onder beheer van de ondertekenaar staan, zo constateren de leden van de D66-fractie. Volgens de regering biedt de verordening hiervoor ruimte, maar stelt als voorwaarde voor een geavanceerde elektronische handtekening dat de ondertekenaar de aanmaakgegevens met een hoog vertrouwensniveau onder zijn uitsluitende controle kan gebruiken. Kan de regering dit nader toelichten?

8. Gegevensbescherming

De leden van de VVD-fractie lezen op pagina 32 van de memorie van toelichting dat het feitelijk beheer van het knooppunt kan worden uitbesteed aan een derde partij. Dit kan bijvoorbeeld aan een partij uit Idensys, het in ontwikkeling zijnde nationaal stelsel voor elektronische identificatie en authenticatie van burgers en bedrijven. Hierbij zal een bewerkersovereenkomst worden gesloten tussen de verantwoordelijke Minister en de beheerder(s). De regering tekent daarbij aan dat het technisch mogelijk is om als lidstaat meerdere knooppunten bij verschillende makelaars van Idensys te implementeren. Deze leden vragen of een toenemend aantal knooppunten niet leidt tot een verzwakking van de beveiliging. Kan de regering daar nader op ingaan? Deze leden vragen tevens op welke termijn de aangekondigde aanvullende Privacy Impact Assessments worden uitgevoerd en of deze in alle gevallen vóór of na wijziging van de onderliggende wetten worden uitgevoerd.

De leden van de SP-fractie lezen in het wetsvoorstel dat met een «bewerkersovereenkomst» het beheer van het knooppunt aan een derde kan worden uitbesteed. Deze leden zijn benieuwd naar de voorzorgsmaatregelen die de regering zal nemen om de bescherming van persoonsgegevens te waarborgen in het geval gekozen gaat worden voor beheer door een private partij. Ook willen deze leden weten hoe tot een dergelijke keuze zal worden gekomen en op welke wijze de Kamer daarbij betrokken wordt. Deze leden zijn tevens benieuwd naar in hoeverre, als dit knooppunt wordt beheerd door een Idensys-partij, de Minister van Binnenlandse Zaken betrokken zal worden bij beperking en oplossing van ontstane problemen. Tevens wijzen deze leden op het commentaar van het Cbp en geven de regering graag mee dat hierin met klem wordt benadrukt dat de Minister van Economische Zaken in alle gevallen primair verantwoordelijk blijft voor het knooppunt en de beveiliging daarvan. Deze leden lezen in het wetsvoorstel ook dat per incident bekeken zal

worden welke maatregelen nodig zijn, vermoedelijk om ontstane problemen op te lossen. Deze leden zijn benieuwd of in het geval van bijvoorbeeld identiteitsdiefstal of het doorgeleiden van verkeerde gegevens protocollen zullen worden opgesteld om problemen zo snel mogelijk te beperken en op te lossen.

De leden van de CDA-fractie vragen de regering of zij kan toelichten op welke wijze in dit wetsvoorstel de privacy wordt gewaarborgd bij de verwerking van persoonsgegevens. Ook vragen deze leden of regering bereid is om de aangekondigde aanvullende Privacy Impact Assessments naar de Kamer te sturen nadat deze is uitgevoerd. Tevens vragen deze leden of de regering kan toelichten waarom elektronische identificatie geldt bij zowel natuurlijk personen als bij rechtspersonen.

8.1 Gegevensbescherming

De leden van de PVV-fractie maken zich zorgen over het eIDAS-knooppunt en de privacy van Nederlandse burgers. De leden zouden graag een uitputtende lijst ontvangen waar deze elektronische identificatie uitruildienst voor benut wordt. Klopt het dat Nederlandse openbare instanties zonder dat een betreffende persoon daarvan op de hoogte is gegevens over de elektronische identiteit kan versturen naar andere EU-lidstaten? Zo ja, zijn er behoudens criminele activiteiten nog meer zaken waar dit voor benut wordt? Op welke wijze is de Nederlandse burger gebaat met deze uitwisseling van elektronische gegevens binnen EU-lidstaten zonder diens persoonlijke toestemming? Verder stelt de regering dat lidstaten verplicht zijn elkaar te informeren over incidenten met de elektronische identiteiten van burgers en bedrijven, maar dat het aan betreffende lidstaat zelf is om te bepalen of de betreffende burger of het bedrijf geïnformeerd wordt over het incident met zijn elektronische identiteit. Kan de regering aangeven welke redenen er zouden kunnen zijn om burgers of bedrijven hier niet over te informeren? Welke andere reden zou er kunnen zijn dan omwille van de publieke opinie incidenten met het Europese elektronische identiteiten systeem niet kenbaar te maken aan betreffende personen of bedrijven? In hoeverre wordt de Kamer geïnformeerd over deze vertrouwensbreuken in dit elektronische identiteiten knooppunt?

8.2 Uitvoeringsmaatregelen

De leden van de D66-fractie stellen vast dat het waarborgen van de integriteit van de door te geven gegevens onderdeel is van het knooppunt. De regering schrijft dat hiertoe maatregelen in het kader van bescherming van persoonsgegevens en informatiebeveiliging zullen worden getroffen. Kan de regering aangeven welke maatregelen hier bedoeld worden?

De regering geeft, tot genoegen van deze leden, aan dat het advies van het Cbp wordt opgevolgd en dat er in het kader van de ontwikkeling van het knooppunt aanvullende Privacy Impact Assessments worden uitgevoerd. De regering schrijft dat situaties als storingen en identiteitsdiefstal zoveel mogelijk door «adequate beveiliging» voorkomen dient te worden. Kan de regering «adequate beveiliging» definiëren? Welke stappen zijn al gezet om deze adequate beveiliging te realiseren, naast de verschillende maatregelen die al genoemd worden?

10. Administratieve lasten en verdere effecten voor het bedrijfsleven

De regering schrijft dat de bepalingen uit de verordening gevolgen kunnen hebben voor de administratieve lasten van aanbieders van vertrouwensdiensten. De regering geeft daarvan echter geen kwantitatieve onderbouwing, omdat dat nog niet mogelijk is. De leden van de VVD-fractie willen de regering oproepen om de toekomstige lasten die uit dit wetsvoorstel en de verordening voortvloeien nauwkeuring in de gaten te houden en er daarbij op in te zetten dat de lasten zo laag mogelijk zijn. Is de regering daartoe bereid, zo vragen deze leden.

De leden van de CDA-fractie vragen de regering om cijfermatig aan te geven hoe groot de toename van de administratieve lasten is voor aanbieders van vertrouwensdiensten en overheden door dit wetsvoorstel. Waaruit bestaat de door de regering verwachte stijging van administratieve lasten voor aanbieders van gekwalificeerde vertrouwensdiensten als gevolg van de verbreding van de scope van de verordening, de vertrouwenslijst en de meldplicht? Deze leden vragen de regering daarnaast welke extra verplichtingen het wetsvoorstel teweegbrengt voor het midden- en kleinbedrijf.

10.1 Elektronische identiteiten

De leden van de D66-fractie constateren dat de private sector niet verplicht is om zich aan te sluiten bij de verplichte erkenning van elektronische identiteiten uit andere lidstaten, maar dat dit wel mogelijk is. Kan de regering nader ingaan op de gevolgen voor de wetswijziging voor de private sector?
Bovenstaande vraag past in een grotere vraag die leeft bij deze leden. De regering schrijft al in de inleiding dat het doel van de verordening is om de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne markt van de Europese Unie te verhogen. Kan de regering ingaan op de verschillen tussen de effecten van deze verordening voor de publieke sector en de private sector? Wat zijn de belangrijkste verschillen?

10.3 Toezichtlasten

De leden van de CDA-fractie vragen de regering of door middel van het wetsvoorstel de rol van de toezichthouder dient te worden uitgebreid. Zo ja, welke kosten brengt dit met zich mee?

De leden van de PVV-fractie constateren dat er nog weinig bekend is over de gevolgen voor de toezichtlasten, behalve dat deze zullen stijgen. Kan de regering aangeven wanneer hier meer duidelijkheid over kan worden verschaft? Is de regering bereid de verdere behandeling van dit wetsvoorstel op te schorten totdat er een compleet beeld is van de financiële impact van dit wetsvoorstel?

De regering schrijft dat er in Nederland momenteel vier private partijen en drie overheidsorganisaties zijn die gekwalificeerde vertrouwensdiensten leveren, zo constateren de leden van de D66-fractie. Daarnaast geeft de regering aan dat het onbekend is in hoeverre deze partijen gekwalificeerde diensten naast de elektronische handtekening gaan aanbieden. Deze leden vragen de regering toe te lichten welke private partijen en overheidsorganisaties bedoeld worden. Wanneer wordt bekend in hoeverre deze partijen gekwalificeerde diensten gaan aanbieden?

11. Financiële gevolgen voor medeoverheden

De leden van de CDA-fractie lezen dat het Ministerie van Economische Zaken in 2018 extra kosten voor medeoverheden via het Gemeente- en Provinciefonds zal compenseren, conform de verplichtingen uit de Financiële Verhoudingswet. Om welke kosten gaat het en kan de regering verzekeren dat er geen bezuiniging zal plaatsvinden op de compensatie die plaats gaat vinden via het Gemeente- en Provinciefonds? Deze leden lezen verder dat het Rijk de extra kosten voor de waterschappen niet zal compenseren, omdat dit niet staat in de Financiële Verhoudingswet of de code interbestuurlijke verhoudingen. De regering verwijst de Waterschappen door naar een Europees proefproject, waardoor de aansluiting via de «Connecting Europe Facility» met Europese middelen zouden kunnen worden gefinancierd. Zou de regering kunnen aangeven welke voorwaarden hieraan verbonden zijn en in hoeverre dit haalbaar is?

13. Internetconsultatie

De leden van de CDA-fractie lezen dat in de internetconsultatie is opgemerkt dat wetgeving niet altijd de meest effectieve manier is om spanningsvelden tussen security en privacy op te lossen. Zou de regering kunnen aangeven in hoeverre overwogen is om bepaalde spanningsvelden tussen security en privacy op andere manieren op te lossen in plaats van met wetgeving?

De leden van de PvdA-fractie vragen waarom is de toepassing van artikel 12 van de Wet raadgevend referendum alsnog is geschrapt na het advies van de Raad van State. Welke volkenrechtelijke organisatie wordt hier bedoeld? Is de Europese Commissie als zodanig op te vatten? Indien de Europese Commissie als zodanig gezien wordt, dan zouden er toch heel veel wetten niet meer onder de Wet raadgevend referendum vallen? Hoe verhoudt zich dit dan tot het referendum over het Associatieverdrag met Oekraïne?
Deze leden vragen waarom waterschappen niet gecompenseerd voor extra kosten. Waarom worden zij verwezen naar de «Connecting Europe Facility»? Zijn de provincies en gemeenten tevreden over de aan hen aangeboden compensatie? Hebben de decentrale overheden Idensys inmiddels goed in beeld?
Tevens vragen deze leden hoe dit wetsvoorstel zich verhoudt tot de bredere Digitale Interne Markt. Wanneer zullen de volgende wetsvoorstellen hierover ingediend worden?

De regering beschrijft dat Nederland er niet voor kan kiezen om alleen afgifte van een gekwalificeerd certificaat met een elektronisch identificatiemiddel van het niveau «hoog» toe te staan. Dit baart de leden van de D66-fractie zorgen. Er wordt immers tegelijkertijd gesteld dat een openbare instantie geen elektronisch identificatiemiddel hoeft te erkennen dat een lager betrouwbaarheidsniveau heeft dan voor de onlinedienst vereist is. Kan de regering dit ophelderen? Is bovenstaande niet tegenstrijdig? Is het voor Nederland mogelijk om alleen elektronische identificatiemiddelen te erkennen van het niveau «hoog»? Bijvoorbeeld door zelf alleen elektronische identificatiemiddelen aan te melden die het niveau «hoog» hebben? Zo nee, waarom niet? Welke stappen neemt de regering in dat geval om ervoor te zorgen dat Nederland slechts elektronische identificatiemiddelen erkent van het niveau «hoog»?

II. ARTIKELEN

Artikel V (artikel 2:16 Awb)

De leden van de CDA-fractie lezen dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De rechtsgevolgen van de andere elektronische handtekeningen dienen te worden vastgesteld door het nationale recht. Klopt het dat in Nederland geavanceerde en andere elektronische handtekeningen ook dezelfde rechtsgevolgen kunnen hebben als een handgeschreven handtekening, indien de methode voor ondertekening die gebruikt is voldoende betrouwbaar is gelet op de aard en inhoud van het elektronische bericht en doel waarvoor het is gebruikt? Zo ja, hoe wordt bepaald wat voldoende betrouwbaar is?

De voorzitter van de commissie,
Vermeij

De adjunct-griffier van de commissie,
Kruithof